

**CLAIM AMENDMENTS**

1    1. (Previously Presented) A method for facilitating secure communications among  
2    multicast nodes in a telecommunications network, the method comprising the  
3    computer-implemented steps of:  
4       receiving, at an authoritative node from a first node, a first request to store an  
5       encryption key, wherein the first request includes an identifier, and wherein  
6       the first node uses the encryption key to encrypt data that is multicast with the  
7       identifier to a plurality of second nodes;  
8       in response to the first request,  
9           the authoritative node storing the encryption key;  
10      the authoritative node creating and storing an association between the  
11           encryption key and the identifier;  
12      receiving, at the authoritative node from at least one second node of the plurality of  
13      second nodes, a second request to obtain the encryption key, wherein the  
14      second request includes the identifier;  
15      in response to the second request,  
16           based on the identifier included in the second request and the association  
17           between the encryption key and the identifier, the authoritative node  
18           retrieving the encryption key; and  
19           the authoritative node sending the encryption key to the at least one second  
20           node for use in decrypting the encrypted data.

1    2. (Previously Presented) A method as recited in Claim 1, wherein:  
2       the authoritative node is a trusted third party performs the steps of receiving the first  
3       request, storing the encryption key, creating and storing the association,  
4       receiving the second request, retrieving the encryption key, and sending the  
5       encryption key;  
6       the first request is encrypted based on a first public key that is associated with the  
7       trusted third party;  
8       the first request is signed with a first private key that is associated with the first node;

9           the first node is a router that acts as a multicast originator;  
10          the plurality of second nodes is a plurality of routers that act as multicast receivers;  
11          the trusted third party is selected from the group consisting of a certificate authority, a  
12               key distribution center, a key exchange authority, and a key exchange center;  
13          the encryption key is selected from the group consisting of a second private key, a  
14               shared key, a pseudo-random string of bits, and a pseudo-random string of  
15               characters; and  
16          the method further comprises the computer-implemented steps of:  
17               prior to sending the encryption key,  
18                   encrypting the encryption key based on a second public key that is  
19                       associated with the at least one second node; and  
20               signing the encrypted encryption key with a third private key that is  
21                       associated with the trusted third party.

1     3. – 5. (Cancelled)

2     6.    (Previously Presented) A method as recited in Claim 1, further comprising the  
3           computer-implemented steps of:  
4           registering a certificate that includes the encryption key and the identifier;  
5           in response to the first request, associating an expiration time with the encryption key;  
6           in response to the second request, determining based on the expiration time whether  
7               the encryption key has expired; and  
8           when the encryption key has expired, revoking the certificate.

1     7. – 8. (Cancelled)

1     9.    (Previously Presented) A method as recited in Claim 1, further comprising the  
2           computer-implemented step of:  
3           generating the encryption key based on an Internet key exchange protocol with the  
4               first node.

1 10. (Cancelled)

1 11. (Original) A method as recited in Claim 1, wherein:  
2 the first node uses the encryption key and Internet protocol security (IPsec) to encrypt  
3 the data that is multicast; and  
4 the at least one second node decrypts the encrypted data based on the encryption key  
5 and IPsec.

1 12. (Previously Presented) A method as recited in Claim 1, further comprising the  
2 computer-implemented steps of:  
3 storing a first list of nodes;  
4 in response to the first request, determining whether the first node is included in the  
5 first list of nodes;  
6 when the first node is included in the first list of nodes, performing the steps of  
7 storing the encryption key and creating and storing the association between the  
8 encryption key and the identifier;  
9 in response to the first request, storing a second list of nodes;  
10 in response to the second request, determining whether the at least one second node is  
11 included in the second list of nodes; and  
12 when the at least one second node is included in the second list of nodes, performing  
13 the steps of retrieving and sending the encryption key.

1 13. – 14. (Cancelled)

1 15. (Original) A method as recited in Claim 1, wherein the encryption key is an old  
2 encryption key, the identifier is an old identifier, and the association is an old  
3 association, and further comprising the steps of:  
4 in response to the first request, associating one or more criteria with the encryption  
5 key;

6           in response to the second request, determining based on the one or more criteria  
7               whether the encryption key is valid; and  
8           when the encryption key is not valid,  
9               receiving a third request to store a new encryption key, wherein the third  
10              request includes a new identifier, and wherein the new encryption key  
11              is used to encrypt additional data that is multicast with the new  
12              identifier to the plurality of second nodes;  
13           in response to the third request,  
14               storing the new encryption key;  
15               creating and storing a new association between the new encryption key  
16              and the new identifier;  
17           receiving, from at least one additional second node of the plurality of second  
18              nodes, a fourth request to obtain the new encryption key, wherein the  
19              fourth request includes the new identifier;  
20           in response to the fourth request,  
21               based on the new identifier included in the fourth request and the new  
22              association between the new encryption key and the new  
23              identifier, retrieving the new encryption key; and  
24               sending the new encryption key to the at least one additional second  
25              node for use in decrypting the encrypted data.

1     16.    (Cancelled)

1     17.    (Original) A method as recited in Claim 1,  
2           wherein:  
3               the identifier is a session identifier;  
4               the encrypted data is multicast with an originator identifier that is based on an  
5              identity of the first node;  
6               the second request includes an unverified originator identifier; and  
7               further comprising the computer-implemented steps of:

8                   in response to the first request, associating the originator identifier with the  
9                   session identifier; and  
10                  in response to the second request, determining whether the unverified  
11                  originator identifier is valid based on the originator identifier and  
12                  informing the at least one second node whether the unverified  
13                  originator is valid.

1 18. - 19. (Cancelled)

1    20. (Original) A method as recited in Claim 1, wherein the identifier is selected from the  
2       group consisting of a hostname, an Internet protocol address, a media access control  
3       address, an Internet security protocol security parameter index, a first string of  
4       pseudo-random bits, a second string of pseudo-random characters, a third string of  
5       arbitrary bits, and a fourth string of arbitrary characters.

1    21. (CURRENTLY AMENDED) A method for encrypting communications among  
2    multicast nodes in a telecommunications network, the method comprising the  
3    computer-implemented steps of:  
4    an originating node sending a first request to store an encryption key and an identifier  
5    ~~that is associated with the encryption key~~ to an authoritative node;  
6    wherein the authoritative node, that in response to the first request, (a) stores  
7    the encryption key ~~and identifier~~ and ~~that (b)~~ creates and stores an  
8    association between ~~the encryption~~ the encryption key and the  
9    identifier;  
10   the originating node encrypting data based on the encryption key; and  
11   the originating node multicasting the encrypted data with the identifier to one or more  
12   receiving nodes, wherein:

13           at least one receiving node of the one or more receiving nodes (a) sends a  
14           second request to obtain the encryption key use the identifier to  
15           retrieve the encryption key from to the authoritative node, wherein the  
16           second request includes the identifier, and (b) decrypts the encrypted  
17           data based on the encryption key that the at least one receiving node  
18           receives from the authoritative node; and  
19           the authoritative node, in response to the second request, (a) retrieves the  
20           encryption key, based on the identifier included in the second request  
21           and the association between the encryption key and the identifier, and  
22           (b) sends the encryption key to the at least one receiving node for use  
23           in decrypting the encrypted data.

1       22. (CURRENTLY AMENDED) A method for decrypting encrypted communications  
2       among multicast nodes in a telecommunications network, the method comprising the  
3       computer-implemented steps of:  
4           a receiving node receiving from an originating node a multicast that includes  
5           encrypted data and an identifier, wherein:  
6           the encrypted data is encrypted by the originating node based on an encryption  
7           key;  
8           the authoritative node receives a first request from the originating node to  
9           store the encryption key, wherein the first request includes an  
10           identifier;  
11           in response to the first request, the authoritative node (a) stores the encryption  
12           key and (b) creates and stores an association between the encryption  
13           key and the identifier;  
14           the receiving node identifying the identifier from the multicast;  
15           the receiving node sending a second request to obtain the encryption key that includes  
16           the identifier to an the authoritative node for to obtain an encryption key used  
17           by the originating node to encrypt the encrypted data, wherein:

18           the authoritative node, in response to the second request, (a) retrieves the  
19           encryption key, based on the identifier included in the second request  
20           and the association between the encryption key and the identifier, and  
21           (b) sends the encryption key for use in decrypting the encrypted data;  
22           in response to sending the second request to the authoritative node, the receiving node  
23           receiving the encryption key; and  
24           the receiving node decrypting the encrypted data based on the encryption key.

1       23. (Original) A method for a certificate authority to facilitate communications based on  
2           Internet protocol security (IPsec) among multicast nodes in a telecommunications  
3           network, the method comprising the computer-implemented steps of:  
4           receiving, at the certificate authority from a first router that acts as a multicast  
5           originator, a first request to register an encryption key, wherein the first  
6           request includes a multicast session identifier and a list of authorized multicast  
7           receivers, and wherein the first router uses the encryption key to encrypt data  
8           based on IPsec and multicasts the encrypted data with the multicast session  
9           identifier to a plurality of second routers that act as multicast receivers;  
10          in response to the first request, the certificate authority creating and storing a  
11           multicast session certificate that includes the encryption key, the multicast  
12           session identifier, and the list of authorized multicast receivers;  
13          receiving, at the certificate authority from at least a particular second router of the  
14           plurality of second routers, a second request to obtain the encryption key,  
15           wherein the second request includes the multicast session identifier;  
16          in response to the second request,  
17           determining whether the particular second router is included in the list of  
18           authorized multicast receivers;  
19           when the particular second router is included in the list of authorized multicast  
20           receivers,  
21           based on the multicast session identifier included in the second request  
22           and the multicast session certificate, the certificate authority  
23           retrieving the encryption key; and

the certificate authority sending the encryption key to the particular second router for use in decrypting the encrypted data based on IPsec.

1    24. (Previously Presented) A computer-readable storage medium carrying one or more  
2    sequences of instructions for facilitating secure communications among multicast  
3    nodes in a telecommunications network, which instructions, when executed by one or  
4    more processors, cause the one or more processors to carry out the steps of:  
5    receiving, at an authoritative node from a first node, a first request to store an  
6    encryption key, wherein the first request includes an identifier, and wherein  
7    the first node uses the encryption key to encrypt data that is multicast with the  
8    identifier to a plurality of second nodes;  
9    in response to the first request,  
10      the authoritative node storing the encryption key;  
11      the authoritative node creating and storing an association between the  
12           encryption key and the identifier;  
13    receiving, at the authoritative node from at least one second node of the plurality of  
14    second nodes, a second request to obtain the encryption key, wherein the  
15    second request includes the identifier;  
16    in response to the second request,  
17      based on the identifier included in the second request and the association  
18           between the encryption key and the identifier, the authoritative node  
19           retrieving the encryption key; and  
20      the authoritative node sending the encryption key to the at least one second  
21           node for use in decrypting the encrypted data.

1       25. (CURRENTLY AMENDED) A computer-readable storage medium carrying one or  
2       more sequences of instructions for encrypting communications among multicast  
3       nodes in a telecommunications network, cause the one or more processors to carry out  
4       the steps of:  
5                 an originating node sending a first request to store an encryption key and an identifier  
6                 that is associated with the encryption key to an authoritative node;  
7                 wherein the authoritative node, that in response to the first request, (a) stores  
8                 the encryption key and identifier and that (b) creates and stores an  
9                 association between the encryption key and the identifier;  
10                 the originating node encrypting data based on the encryption key; and  
11                 the originating node multicasting the encrypted data with the identifier to one or more  
12                 receiving nodes, wherein:  
13                 at least one receiving node of the one or more receiving nodes (a) sends a  
14                 second request to obtain the encryption key use the identifier to  
15                 retrieve the encryption key from to the authoritative node, wherein the  
16                 second request includes the identifier, and (b) decrypts the encrypted  
17                 data based on the encryption key that the at least one receiving node  
18                 receives from the authoritative node; and  
19                 the authoritative node, in response to the second request, (a) retrieves the  
20                 encryption key, based on the identifier included in the second request  
21                 and the association between the encryption key and the identifier, and  
22                 (b) sends the encryption key to the at least one receiving node for use  
23                 in decrypting the encrypted data.

1       26. (Previously Presented) An apparatus for facilitating secure communications among  
2       multicast nodes in a telecommunications network, comprising:  
3       means for receiving, at an authoritative node from a first node, a first request to store  
4       an encryption key, wherein the first request includes an identifier, and wherein  
5       the first node uses the encryption key to encrypt data that is multicast with the  
6       identifier to a plurality of second nodes;  
7       means for the authoritative node storing the encryption key, in response to the first  
8       request;  
9       means for the authoritative node creating and storing an association between the  
10      encryption key and the identifier, in response to the first request;  
11      means for receiving, at the authoritative node from at least one second node of the  
12      plurality of second nodes, a second request to obtain the encryption key,  
13      wherein the second request includes the identifier;  
14      means for the authoritative node retrieving the encryption key, in response to the  
15      second request and based on the identifier included in the second request and  
16      the association between the encryption key and the identifier; and  
17      means for the authoritative node sending the encryption key to the at least one second  
18      node for use in decrypting the encrypted data, in response to the second  
19      request.

1       27. (CURRENTLY AMENDED) An apparatus for encrypting communications among  
2       multicast nodes in a telecommunications network, comprising:  
3       means for an originating node sending a first request to store an encryption key and an  
4       identifier ~~that is associated with the encryption key~~ to an authoritative node;  
5       wherein the authoritative node, that in response to the first request, (a) stores  
6       the encryption key ~~and identifier~~ and that (b) creates and stores an  
7       association between ~~the encryption~~ the encryption key and the  
8       identifier;  
9       means for the originating node encrypting data based on the encryption key; and

10 means for the originating node multicasting the encrypted data with the identifier to  
11 one or more receiving nodes, wherein:  
12 at least one receiving node of the one or more receiving nodes (a) sends a  
13 second request to obtain the encryption key ~~use the identifier to~~  
14 ~~retrieve the encryption key from to~~ the authoritative node, wherein the  
15 second request includes the identifier, and (b) decrypts the encrypted  
16 data based on the encryption key that the at least one receiving node  
17 receives from the authoritative node; and  
18 the authoritative node, in response to the second request, (a) retrieves the  
19 encryption key, based on the identifier included in the second request  
20 and the association between the encryption key and the identifier, and  
21 (b) sends the encryption key to the at least one receiving node for use  
22 in decrypting the encrypted data. the one or more receiving nodes use  
23 the identifier to retrieve the encryption key from the authoritative node  
24 and decrypt the encrypted data based on the encryption key.

1 28. (Previously Presented) An apparatus for facilitating secure communications among  
2 multicast nodes in a telecommunications network, comprising:  
3 a processor;  
4 one or more stored sequences of instructions which, when executed by the processor,  
5 cause the processor to carry out the steps of:  
6 receiving, at an authoritative node from a first node, a first request to store an  
7 encryption key, wherein the first request includes an identifier, and  
8 wherein the first node uses the encryption key to encrypt data that is  
9 multicast with the identifier to a plurality of second nodes;  
10 in response to the first request,  
11 the authoritative node storing the encryption key;  
12 the authoritative node creating and storing an association between the  
13 encryption key and the identifier;

14 receiving, at the authoritative node from at least one second node of the  
15 plurality of second nodes, a second request to obtain the encryption  
16 key, wherein the second request includes the identifier;  
17 in response to the second request,  
18 based on the identifier included in the second request and the  
19 association between the encryption key and the identifier, the  
20 authoritative node retrieving the encryption key; and  
21 the authoritative node sending the encryption key to the at least one  
22 second node for use in decrypting the encrypted data.

1 29. (CURRENTLY AMENDED) An apparatus for encrypting communications among  
2 multicast nodes in a telecommunications network, comprising:  
3 a processor;  
4 one or more stored sequences of instructions which, when executed by the processor,  
5 cause the processor to carry out the steps of:  
6 an originating node sending a first request to store an encryption key and an  
7 identifier ~~that is associated with the encryption key~~ to an authoritative  
8 node;  
9 wherein the authoritative node, that in response to the first request, (a)  
10 stores the encryption key ~~and identifier~~ and ~~that (b)~~ creates and  
11 stores an association between ~~the encryption~~ the encryption key  
12 and the identifier;  
13 the originating node encrypting data based on the encryption key; and  
14 the originating node multicasting the encrypted data with the identifier to one  
15 or more receiving nodes, wherein:

16                   at least one receiving node of the one or more receiving nodes (a)  
17                   sends a second request to obtain the encryption key ~~use the~~  
18                   identifier to retrieve the encryption key from to the  
19                   authoritative node, wherein the second request includes the  
20                   identifier, and (b) decrypts the encrypted data based on the  
21                   encryption key that the at least one receiving node receives  
22                   from the authoritative node; and  
23                   the authoritative node, in response to the second request, (a) retrieves  
24                   the encryption key, based on the identifier included in the  
25                   second request and the association between the encryption key  
26                   and the identifier, and (b) sends the encryption key to the at  
27                   least one receiving node for use in decrypting the encrypted  
28                   data.

1       30. (Previously Presented) An apparatus as recited in Claim 26, wherein:  
2                   the means for receiving the first request, storing the encryption key, creating and  
3                   storing the association, receiving the second request, retrieving the encryption  
4                   key, and sending the encryption key are included in a trusted third party;  
5                   the trusted third party is the authoritative node;  
6                   the first request is encrypted based on a first public key that is associated with the  
7                   trusted third party;  
8                   the first request is signed with a first private key that is associated with the first node;  
9                   the first node is a router that acts as a multicast originator;  
10                  the plurality of second nodes is a plurality of routers that act as multicast receivers;  
11                  the trusted third party is selected from the group consisting of a certificate authority, a  
12                  key distribution center, a key exchange authority, and a key exchange center;  
13                  the encryption key is selected from the group consisting of a second private key, a  
14                  shared key, a pseudo-random string of bits, and a pseudo-random string of  
15                  characters; and  
16                  the apparatus further comprises:

17           means for encrypting, prior to sending the encryption key, the encryption key  
18               based on a second public key that is associated with the at least one  
19               second node; and  
20           means for signing, prior to sending the encryption key, the encrypted  
21               encryption key with a third private key that is associated with the  
22               trusted third party.

1     31. (Previously Presented) An apparatus as recited in Claim 26, further comprising:  
2           means for registering a certificate that includes the encryption key and the identifier;  
3           means for associating, in response to the first request, an expiration time with the  
4               encryption key;  
5           means for determining, in response to the second request, based on the expiration  
6               time whether the encryption key has expired; and  
7           means for revoking the certificate when the encryption key has expired.

1     32. (Previously Presented) An apparatus as recited in Claim 26, further comprising:  
2           means for generating the encryption key based on an Internet key exchange protocol  
3               with the first node.

1     33. (Previously Presented) An apparatus as recited in Claim 26, wherein:  
2           the first node uses the encryption key and Internet protocol security (IPsec) to encrypt  
3               the data that is multicast; and  
4           the at least one second node decrypts the encrypted data based on the encryption key  
5               and IPsec.

1     34. (Previously Presented) An apparatus as recited in Claim 26, further comprising:  
2           means for storing a first list of nodes;  
3           means for determining, in response to the first request, whether the first node is  
4               included in the first list of nodes;

5 means for causing, when the first node is included in the first list of nodes, the storing  
6 of the encryption key and the creating and storing of the association between  
7 the encryption key and the identifier;  
8 means for storing, in response to the first request, a second list of nodes;  
9 means for determining, in response to the second request, whether the at least one  
10 second node is included in the second list of nodes; and  
11 means for causing, when the at least one second node is included in the second list of  
12 nodes, the retrieving and sending of the encryption key.

1 35. (Previously Presented) An apparatus as recited in Claim 26, wherein the encryption  
2 key is an old encryption key, the identifier is an old identifier, and the association is  
3 an old association, and further comprising:  
4 means for associating, in response to the first request, one or more criteria with the  
5 encryption key;  
6 means for determining, in response to the second request, based on the one or more  
7 criteria whether the encryption key is valid;  
8 means for receiving, when the encryption key is not valid, a third request to store a  
9 new encryption key, wherein the third request includes a new identifier, and  
10 wherein the new encryption key is used to encrypt additional data that is  
11 multicast with the new identifier to the plurality of second nodes;  
12 means for storing, in response to the third request, the new encryption key;  
13 means for creating and storing, in response to the third request, a new association  
14 between the new encryption key and the new identifier;  
15 means for receiving, from at least one additional second node of the plurality of  
16 second nodes, a fourth request to obtain the new encryption key, wherein the  
17 fourth request includes the new identifier;  
18 means for retrieving, in response to the fourth request, the new encryption key, based  
19 on the new identifier included in the fourth request and the new association  
20 between the new encryption key and the new identifier; and  
21 means for sending, in response to the fourth request, the new encryption key to the at  
22 least one additional second node for use in decrypting the encrypted data.

1       36. (Previously Presented) An apparatus as recited in Claim 26,  
2           wherein:  
3                  the identifier is a session identifier;  
4                  the encrypted data is multicast with an originator identifier that is based on an  
5                           identity of the first node;  
6                  the second request includes an unverified originator identifier; and  
7                  further comprising:  
8                          means for associating, in response to the first request, the originator identifier  
9                                   with the session identifier; and  
10                          means for determining, in response to the second request, whether the  
11                                   unverified originator identifier is valid based on the originator  
12                                   identifier and informing the at least one second node whether the  
13                                   unverified originator is valid.

1       37. (Previously Presented) An apparatus as recited in Claim 26, wherein the identifier is  
2           selected from the group consisting of a hostname, an Internet protocol address, a  
3           media access control address, an Internet security protocol security parameter index, a  
4           first string of pseudo-random bits, a second string of pseudo-random characters, a  
5           third string of arbitrary bits, and a fourth string of arbitrary characters.

1       38. (Previously Presented) An apparatus as recited in Claim 28, wherein:  
2           the apparatus is part of a trusted third party;  
3           the trusted third party is the authoritative node;  
4           the first request is encrypted based on a first public key that is associated with the  
5                           trusted third party;  
6           the first request is signed with a first private key that is associated with the first node;  
7           the first node is a router that acts as a multicast originator;  
8           the plurality of second nodes is a plurality of routers that act as multicast receivers;  
9           the trusted third party is selected from the group consisting of a certificate authority, a  
10                           key distribution center, a key exchange authority, and a key exchange center;

11           the encryption key is selected from the group consisting of a second private key, a  
12           shared key, a pseudo-random string of bits, and a pseudo-random string of  
13           characters; and  
14           the apparatus further comprises one or more stored sequences of instructions which,  
15           when executed by the processor, cause the processor to carry out the steps of:  
16           prior to sending the encryption key,  
17                 encrypting the encryption key based on a second public key that is  
18                 associated with the at least one second node; and  
19                 signing the encrypted encryption key with a third private key that is  
20                 associated with the trusted third party.

1       39. (Previously Presented) An apparatus as recited in Claim 28, further comprising one or  
2       more stored sequences of instructions which, when executed by the processor, cause  
3       the processor to carry out the steps of:  
4       registering a certificate that includes the encryption key and the identifier;  
5       in response to the first request, associating an expiration time with the encryption key;  
6       in response to the second request, determining based on the expiration time whether  
7                 the encryption key has expired; and  
8       when the encryption key has expired, revoking the certificate.

1       40. (Previously Presented) An apparatus as recited in Claim 28, further comprising one or  
2       more stored sequences of instructions which, when executed by the processor, cause  
3       the processor to carry out the step of:  
4       generating the encryption key based on an Internet key exchange protocol with the  
5                 first node.

1       41. (Previously Presented) An apparatus as recited in Claim 28, wherein:  
2       the first node uses the encryption key and Internet protocol security (IPsec) to encrypt  
3                 the data that is multicast; and  
4       the at least one second node decrypts the encrypted data based on the encryption key  
5                 and IPsec.

1       42. (Previously Presented) An apparatus as recited in Claim 28, further comprising one or  
2       more stored sequences of instructions which, when executed by the processor, cause  
3       the processor to carry out the steps of:  
4              storing a first list of nodes;  
5              in response to the first request, determining whether the first node is included in the  
6              first list of nodes;  
7              when the first node is included in the first list of nodes, performing the steps of  
8                  storing the encryption key and creating and storing the association between the  
9                  encryption key and the identifier;  
10             in response to the first request, storing a second list of nodes;  
11             in response to the second request, determining whether the at least one second node is  
12              included in the second list of nodes; and  
13             when the at least one second node is included in the second list of nodes, performing  
14              the steps of retrieving and sending the encryption key.

1       43. (Previously Presented) An apparatus as recited in Claim 28, wherein the encryption  
2       key is an old encryption key, the identifier is an old identifier, and the association is  
3       an old association, and further comprising one or more stored sequences of  
4       instructions which, when executed by the processor, cause the processor to carry out  
5       the steps of:  
6              in response to the first request, associating one or more criteria with the encryption  
7              key;  
8              in response to the second request, determining based on the one or more criteria  
9              whether the encryption key is valid; and  
10             when the encryption key is not valid,  
11                  receiving a third request to store a new encryption key, wherein the third  
12                  request includes a new identifier, and wherein the new encryption key  
13                  is used to encrypt additional data that is multicast with the new  
14                  identifier to the plurality of second nodes;  
15             in response to the third request,



1    45. (Previously Presented) An apparatus as recited in Claim 28, wherein the identifier is  
2       selected from the group consisting of a hostname, an Internet protocol address, a  
3       media access control address, an Internet security protocol security parameter index, a  
4       first string of pseudo-random bits, a second string of pseudo-random characters, a  
5       third string of arbitrary bits, and a fourth string of arbitrary characters.